



MoGua

德信 1.10.5.APK 分析报告



APP名称:	德信
包名:	com.dexin.dzapp
域名线索:	50条
URL线索:	73条
邮箱线索:	6条
分析日期:	2025年7月8日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: d4eaf068c5f24c428421f1d9bbc05c42.apk
文件大小: 120.02MB
MD5值: 17981d893abfa99738ccb32fcaf0506f
SHA1值: dc7810867649ab0613373d480206a22e71667a6d
SHA256值: 1fcbbf14b09e40ed650f5bcd933875f40a6e2520c10ebad6c6ae12b03d3f1553

i APP 信息

App名称: 德信
包名: com.dexin.dzapp
主活动Activity: com.dexin.dzpk.MainActivity
安卓版本名称: 1.10.5
安卓版本: 4128

域名线索

域名	服务器信息
api.dw3.app	没有服务器地理信息.
www.example.com	IP: 93.184.215.14 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052570 经度: -118.243904
schemas.android.com	没有服务器地理信息.
	IP: 101.72.254.86

playvideo.qcloud.com	所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
htapi.qvxxm8m.com	IP: 213.176.107.21 所属国家: Iran (Islamic Republic of) 地区: Tehran 城市: Tehran 纬度: 35.694241 经度: 51.421310
stackoverflow.com	IP: 104.18.32.7 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
htapi.sgqntk1.com	IP: 213.176.85.56 所属国家: Iran (Islamic Republic of) 地区: Tehran 城市: Tehran 纬度: 35.694241 经度: 51.421310
www.gnu.org	IP: 209.51.188.116 所属国家: United States of America 地区: Massachusetts 城市: Somerville 纬度: 42.387600 经度: -71.099503
www.xxxx.com	IP: 54.153.216.130 所属国家: Australia 地区: New South Wales 城市: Sydney 纬度: -33.867779 经度: 151.207047
www.googleapis.com	IP: 142.251.8.95 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
prehtapi.idplj4pe.com	IP: 18.180.43.140 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
api.dw2.app	没有服务器地理信息.
	IP: 172.66.40.222 所属国家: United States of America 地区: California

www.codeandweb.com	城市: San Francisco 纬度: 37.775700 经度: -122.395203
www.aseprite.org	IP: 107.178.219.96 所属国家: United States of America 地区: Iowa 城市: Council Bluffs 纬度: 41.261940 经度: -95.860832
github.com	IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
alifei01.cfp.cn	IP: 182.40.59.224 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941
api.dw5.app	没有服务器地理信息.
api.dw10.app	没有服务器地理信息.
tenfei05.cfp.cn	IP: 123.126.74.135 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
api.dw6.app	没有服务器地理信息.
www.sophotio.com	IP: 169.254.254.254 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
img2.baidu.com	IP: 119.188.176.35 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223
en.wikipedia.org	IP: 198.35.26.96 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.791256 经度: -122.400810

developer.android.com	IP: 142.251.8.102 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
htapi.octogenfy.com	IP: 213.176.107.55 所属国家: Iran (Islamic Republic of) 地区: Tehran 城市: Tehran 纬度: 35.694241 经度: 51.421310
logs.go.uploadlog.com	没有服务器地理信息.
api.dw8.app	没有服务器地理信息.
www.googleapis.cn	IP: 114.250.69.34 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
www.a339efi.com	没有服务器地理信息.
alifei02.cfp.cn	IP: 175.22.52.225 所属国家: China 地区: jilin 城市: Changchun 纬度: 43.880001 经度: 125.322777
ifconfig.co	IP: 172.67.168.106 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
api.dw7.app	没有服务器地理信息.
vodreport.qcloud.com	IP: 123.125.46.250 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
api.dw9.app	没有服务器地理信息.
api.dw4.app	没有服务器地理信息.
htapi.sverou.com	IP: 213.176.107.24 所属国家: Iran (Islamic Republic of) 地区: Tehran 城市: Tehran

	纬度: 35.694241 经度: 51.421310
www.tensorflow.org	IP: 142.251.8.100 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
api.dw13.app	没有服务器地理信息.
api.flutter.dev	IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
dev.w3.org	IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
developer.mozilla.org	IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
ns.adobe.com	没有服务器地理信息.
1255566655.vod2.myqcloud.com	IP: 218.29.50.120 所属国家: China 地区: Henan 城市: Xinxiang 纬度: 35.308777 经度: 113.867203
cloud.tencent.com	IP: 123.6.40.212 所属国家: China 地区: Henan 城市: Zhengzhou 纬度: 34.757778 经度: 113.648613
api.dw12.app	没有服务器地理信息.
paulbakaus.com	IP: 167.172.18.193 所属国家: United States of America 地区: New Jersey 城市: Clifton 纬度: 40.858585 经度: -74.163605
api.dw11.app	没有服务器地理信息.

htapi.sophotio.com	IP: 124.239.251.60 所属国家: China 地区: Hebei 城市: Shijiazhuang 纬度: 38.041599 经度: 114.478081
47.75.218.191	IP: 47.75.218.191 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
api.dw1.app	没有服务器地理信息.

 URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	b1/k.java
https://github.com/Baseflow/flutter-permission-handler/issues	com/baseflow/permissionhandler/PermissionManager.java
https://api.dw1.app/	com/bw/tmapmanager/domains/config/TmapDomainsConfig.java
https://api.dw2.app/	com/bw/tmapmanager/domains/config/TmapDomainsConfig.java
https://api.dw3.app/	com/bw/tmapmanager/domains/config/TmapDomainsConfig.java
https://api.dw4.app/	com/bw/tmapmanager/domains/config/TmapDomainsConfig.java
https://api.dw5.app/	com/bw/tmapmanager/domains/config/TmapDomainsConfig.java
https://api.dw6.app/	com/bw/tmapmanager/domains/config/TmapDomainsConfig.java
https://api.dw7.app/	com/bw/tmapmanager/domains/config/TmapDomainsConfig.java
https://api.dw8.app/	com/bw/tmapmanager/domains/config/TmapDomainsConfig.java
https://api.dw9.app/	com/bw/tmapmanager/domains/config/TmapDomainsConfig.java
https://api.dw10.app/	com/bw/tmapmanager/domains/config/TmapDomainsConfig.java
https://api.dw11.app/	com/bw/tmapmanager/domains/config/TmapDomainsConfig.java
https://api.dw12.app/	com/bw/tmapmanager/domains/config/TmapDomainsConfig.java
https://api.dw13.app/	com/bw/tmapmanager/domains/config/TmapDomainsConfig.java

https://ifconfig.co/json	com/bw/tmapmanager/utis/SDKTools.java
http://www.example.com	com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/CustomTabsHelper.java
https://cloud.tencent.com/act/event/License	com/tencent/liteav/a.java
https://vodreport.qcloud.com/describeControllInfos/v1/	com/tencent/liteav/txcvodplayer/a/b.java
http://playvideo.qcloud.com/getplayinfo/v2	com/tencent/liteav/txcvodplayer/b/d.java
https://playvideo.qcloud.com/getplayinfo/v2	com/tencent/liteav/txcvodplayer/b/d.java
http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/coverBySnapshot/1513156403_1311093072.100_0.jpg?t=5c08d9fa&us=someus&sign=95f34beb353fe32cfe7f8b5e79cc28b1\	com/tencent/liteav/txcvodplayer/b/d.java
http://1255566655.vod2.myqcloud.com/ca754badvodgzp1255566655/8f5fbff14564972818519602447/imageSprite/1513156058_533711271_00001.jpg?t=5c08d9fa&us=someus&sign=79449db4e1fb05a3becfa096613659c3\	com/tencent/liteav/txcvodplayer/b/d.java
http://1255566655.vod2.myqcloud.com/ca754badvodgzp1255566655/8f5fbff14564972818519602447/imageSprite/1513156058_533711271.vtt?t=5c08d9fa&us=someus&sign=79449db4e1fb05a3becfa096613659c3\	com/tencent/liteav/txcvodplayer/b/d.java
http://1255566655.vod2.myqcloud.com/ca754badvodgzp1255566655/8f5fbff14564972818519602447/uAnXX0OMLSAA.wmv?t=5c08d9fa&us=someus&sign=659af5dd3f27eb92dc4ed74eb561daa4\	com/tencent/liteav/txcvodplayer/b/d.java
http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/master_playlist.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\	com/tencent/liteav/txcvodplayer/b/d.java
http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f220.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\	com/tencent/liteav/txcvodplayer/b/d.java
http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f230.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\	com/tencent/liteav/txcvodplayer/b/d.java
http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f240.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\	com/tencent/liteav/txcvodplayer/b/d.java
http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f210.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\	com/tencent/liteav/txcvodplayer/b/d.java
http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f10.mp4?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\	com/tencent/liteav/txcvodplayer/b/d.java
http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f20.mp4?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\	com/tencent/liteav/txcvodplayer/b/d.java
https://playvideo.qcloud.com/getplayinfo/v4	com/tencent/liteav/txcvodplayer/b/c.java
https://www.googleapis.cn/certificateprovisioning/v1/devicecertificates/create?key=AlzaSyB-5OLKTx2iU5mko18DfdwK5611JljbUhE	com/tencent/rtmp/TXPlayerDrmBuilder.java
https://www.googleapis.com/certificateprovisioning/v1/devicecertificates/create?key=AlzaSyB-5OLKTx2iU5mko18DfdwK5611JljbUhE	com/tencent/rtmp/TXPlayerDrmBuilder.java
https://en.wikipedia.org/wiki/Blend_modes\n//	com/tencent/ugc/videoprocessor/transitions/StereoViewerFilter.java
http://logs.go.uploadlog.com:81/	com/tianyu/tyinstall/constant/TYInstallConstant.java

[illegible]

	Mogua Engine V2
https://www.codeandweb.com/texturpacker	Mogua Engine V2
https://www.codeandweb.com/texturpacker	Mogua Engine V2
https://www.codeandweb.com/texturpacker	Mogua Engine V2
https://www.codeandweb.com/texturpacker	Mogua Engine V2
https://www.codeandweb.com/texturpacker	Mogua Engine V2
https://www.codeandweb.com/texturpacker	Mogua Engine V2
https://www.codeandweb.com/texturpacker	Mogua Engine V2
https://www.codeandweb.com/texturpacker	Mogua Engine V2
https://www.codeandweb.com/texturpacker	Mogua Engine V2
https://www.codeandweb.com/texturpacker	Mogua Engine V2
https://www.codeandweb.com/texturpacker	Mogua Engine V2
https://www.codeandweb.com/texturpacker	Mogua Engine V2
https://www.codeandweb.com/texturpacker	Mogua Engine V2
https://www.codeandweb.com/texturpacker	Mogua Engine V2
https://www.codeandweb.com/texturpacker	Mogua Engine V2
https://www.codeandweb.com/texturpacker	Mogua Engine V2
https://www.codeandweb.com/texturpacker	Mogua Engine V2
https://www.codeandweb.com/texturpacker	Mogua Engine V2
https://www.codeandweb.com/texturpacker	Mogua Engine V2
https://www.codeandweb.com/texturpacker	Mogua Engine V2
https://www.codeandweb.com/texturpacker	Mogua Engine V2
https://www.codeandweb.com/texturpacker	Mogua Engine V2
http://www.aseprite.org/	Mogua Engine V2
https://www.codeandweb.com/texturpacker	Mogua Engine V2
https://www.codeandweb.com/texturpacker	Mogua Engine V2
https://www.codeandweb.com/texturpacker	Mogua Engine V2

https://www.codeandweb.com/texturepacker	Mogua Engine V2
https://www.codeandweb.com/texturepacker	Mogua Engine V2
https://www.codeandweb.com/texturepacker	Mogua Engine V2
https://www.codeandweb.com/texturepacker	Mogua Engine V2
https://www.codeandweb.com/texturepacker	Mogua Engine V2
https://www.codeandweb.com/texturepacker	Mogua Engine V2
https://tenfei05.cfp.cn/creative/vcg/veer/800/new/VCG41N864619006.jpg	Mogua Engine V2
https://tenfei05.cfp.cn/creative/vcg/veer/800/new/VCG41N864619006.jpg	Mogua Engine V2
https://alifei01.cfp.cn/creative/vcg/800/new/VCG41N1209502987.jpg	Mogua Engine V2
https://alifei02.cfp.cn/creative/vcg/800/new/VCG211156650833.jpg	Mogua Engine V2
https://tenfei05.cfp.cn/creative/vcg/veer/800/new/VCG41N864619006.jpg	Mogua Engine V2
https://alifei01.cfp.cn/creative/vcg/800/new/VCG41N1209502987.jpg	Mogua Engine V2
https://alifei02.cfp.cn/creative/vcg/800/new/VCG211156650833.jpg	Mogua Engine V2
https://img2.baidu.com/it/u=861869171,3366406111&fm=253&fmt=auto&app=138&f=JPG?w=500&h=500	Mogua Engine V2
https://tenfei05.cfp.cn/creative/vcg/veer/800/new/VCG41N864619006.jpg	Mogua Engine V2
https://alifei01.cfp.cn/creative/vcg/800/new/VCG41N1209502987.jpg	Mogua Engine V2
https://alifei02.cfp.cn/creative/vcg/800/new/VCG211156650833.jpg	Mogua Engine V2
https://alifei02.cfp.cn/creative/vcg/800/new/VCG211156650833.jpg	Mogua Engine V2
http://paulbkaus.com/tutorials/html5/web-audio-on-ios/	Mogua Engine V2
http://stackoverflow.com/questions/24119684	Mogua Engine V2
http://dev.w3.org/html5/spec-author-view/spec.html	Mogua Engine V2
<a data-bbox="117 1242 346 1263" href="https://www.gnu.org/licenses/>.">https://www.gnu.org/licenses/>.	Mogua Engine V2
<a data-bbox="117 1295 346 1317" href="https://www.gnu.org/licenses/>.">https://www.gnu.org/licenses/>.	Mogua Engine V2
<a data-bbox="117 1349 346 1370" href="https://www.gnu.org/licenses/>.">https://www.gnu.org/licenses/>.	Mogua Engine V2
https://github.com/richtr/NoSleep.js/issues/15	Mogua Engine V2
https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released	Mogua Engine V2

https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/arm64-v8a/libapp.so
https://www.tensorflow.org/lite/guide/ops_select	lib/arm64-v8a/libbarhopper_v3.so
http://http	lib/arm64-v8a/libbarhopper_v3.so
https://www.tensorflow.org/lite/guide/ops_custom	lib/arm64-v8a/libbarhopper_v3.so

✉ 邮箱线索

邮箱地址	所在文件
xxx@email.elided	com/tencent/liteav/base/PiiElider.java
invalidname@3x.png	Mogua Engine V2
赢了-金边@3x.png	Mogua Engine V2
赢了-金边@3x.png	Mogua Engine V2
viewsummarymodelimpl@1050145727.fromjson	lib/arm64-v8a/libapp.so
android-sdk-releaser@oqe15.prod	lib/arm64-v8a/libbarhopper_v3.so

☰ 手机线索

手机号	所在文件
14159265358	com/tencent/ugc/videoprocessor/transitions/BounceFilter.java

☼ 签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=123456, ST=ante, L=ante, O=ante, OU=ante, CN=ante
签名算法: rsassa_pkcs1v15
有效期自: 2023-06-24 13:10:01+00:00
有效期至: 2050-11-09 13:10:01+00:00
发行人: C=123456, ST=ante, L=ante, O=ante, OU=ante, CN=ante
序列号: 0x6e63cd0e
哈希算法: sha256
md5值: 3e53a63da9a82e4da82ca7aaae5c9ebd
sha1值: 6f7b600d1197a5e275a53e154ec463f4430b8ba8
sha256值: 69abcce657bb268de03c8120fa50f9b107293def25e04aa0e9a9538a95954c51
sha512值: d116cbd4e5488086dc77337d95ab173ed2080912fd759d339ea5f3793cd548bb593f3918d564186d7fde3962f847745c23331936827dca6c55c93fb36137c79e

公钥算法: rsa
密钥长度: 2048
指纹: ec9900e4ff5db0f7bbcd2c771cefc6446069bef8d22490f0a4316300eb902d6f

🔑 硬编码敏感信息

🔒 加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

🧩 第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

☰ 此APP的危险动作

向手机申请的权限	是否危险	类型	详细情况
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.ACCESS_NETWORK_STATE	正常	查看网络状态	允许应用程序查看所有网络的状态
android.permission.ACCESS_WIFI_STATE	正常	查看Wi-Fi状态	允许应用程序查看有关 Wi-Fi 状态的信息
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储
android.permission.READ_EXTERNAL_STORAGE	危险	读取外部存储器内容	允许应用程序从外部存储读取
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.CAMERA	危险	拍照和录像	允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像
android.permission.READ_PHONE_STATE	危险	读取电话状态和身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等
android.permission.WAKE_LOCK	正常	防止手机睡眠	允许应用程序防止手机进入睡眠状态
android.permission.FOREGROUND_SERVICE	正常		允许当前应用程序使用 Service.startForeground。

android.permission.REQUEST_INSTALL_PACKAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_AUDIO	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许应用程序请求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
android.permission.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
android.permission.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
android.permission.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
com.dexin.dzapp.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.dexin.dzpk.MainActivity	Schemes: dzpkunilinks://, Hosts: item,